

(19) World Intellectual Property  
Organization  
International Bureau



(43) International Publication Date  
24 February 2005 (24.02.2005)

PCT

(10) International Publication Number  
**WO 2005/018185 A1**

(51) International Patent Classification<sup>7</sup>: **H04L 27/26**

(21) International Application Number:  
PCT/IB2004/051378

(22) International Filing Date: 3 August 2004 (03.08.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
03102524.0 13 August 2003 (13.08.2003) EP

(71) Applicant (for DE only): **PHILIPS INTELLECTUAL  
PROPERTY & STANDARDS GMBH** [DE/DE]; Stein-  
damm 94, 20099 Hamburg (DE).

(71) Applicant (for AE, AG, AL, AM, AT, AU, AZ, BA, BB, BE,  
BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CY, CZ,  
DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM,

HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK,  
LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ,  
NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD,  
SE, SG, SK, SL, SY, SZ, TJ, TM, TN, TR, TT, TZ, UA, UG,  
UZ, VC, VN, YU, ZA, ZM, ZW only): **KONINKLIJKE  
PHILIPS ELECTRONICS N. V.** [NL/NL]; Groenewoud-  
seweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors; and

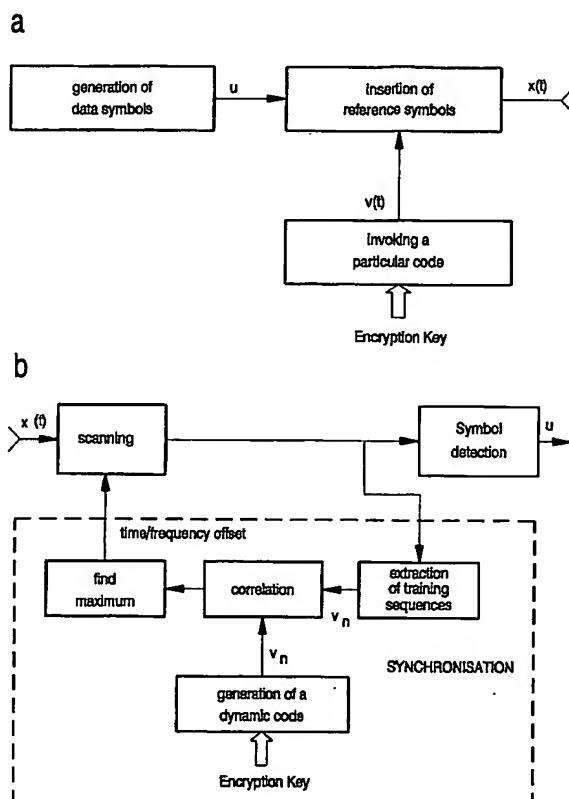
(75) Inventors/Applicants (for US only): **DALMASES,  
Francesc** [ES/DE]; c/o Philips Intellectual Property &  
Standards GmbH, Weissshausstr. 2, 52066 Aachen (DE).  
**KAHLERT, Joachim** [DE/DE]; c/o Philips Intellectual  
Property & Standards GmbH, Weissshausstr. 2, 52066  
Aachen (DE).

(74) Agent: **MEYER, Michael**; Philips Intellectual Property &  
Standards GmbH, Weissshausstr. 2, 52066 Aachen (DE).

(81) Designated States (unless otherwise indicated, for every  
kind of national protection available): AE, AG, AL, AM,  
AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN,

[Continued on next page]

(54) Title: ENCRYPTION METHOD AND DECODING METHOD FOR A DIGITAL TRANSMISSION SYSTEM



(57) Abstract: An encryption method and decoding method for a digital transmission system, in which the digital data stream comprises an alternating sequence of training sequences and data symbols, and the training sequences are dynamically coded. At the receiving end, a decoding code ( $V_n$ ) is generated by a code generator as a function of an encryption key (200). This decoding code is sent to a correlator, where it is mixed with the encryption code  $V_n$  extracted from the digital data stream. The correlator generates a correcting variable to compensate the offset in respect of time or frequency between the sender and receiver. Encryption is achieved through the alteration of the code used during the transmission.



CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**Published:**

— with international search report

**(84) Designated States** (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*